Public Record Office Victoria
Standards and Policy

Recordkeeping Policy

PUBLIC RECORD OFFICE VICTORIA

Cloud Computing: Implications for Records Management

Version Number: 1.0

Issue date: 04/04/2012

Closing for comments: 31/05/2012

Victoria

Acronyms

1 The following acronyms are used throughout the entirety of this document.

ADRI	Australian Digital Recordkeeping Initiative
CRM	Customer Relationship Management
FOI	Freedom of Information
IaaS	Infrastructure as a Service
ICT	Information and Communication Technology
ISP	Internet Service Provider
IT	Information Technology
NIST	National Institute of Science and Technology
PaaS	Platform as a Service
PROS	Public Record Office Standard
PROV	Public Record Office Victoria
RICC	Recordkeeping Implications for Cloud Computing
SLA	Service Level Agreement
VPS	Victorian Public Service

Table of Contents

Copyright Statement

Disclaimer

The State of Victoria gives no warranty that the information in this version is correct or complete, error free or contains no omissions. The State of Victoria shall not be liable for any loss howsoever caused whether due to negligence or otherwise arising from the use of this Guideline.

Use of Terminology

For the purposes of this Issues paper the term data is used to refer to records within a cloud environment. Data means a Public Record as defined in the *Public Records Act 1973* (here after referred to as the act).

Records Management Standards Application

The Recordkeeping Standards apply to all records in all formats, media or systems (including business systems). This Issues Paper identifies records management risks that are specific to cloud computing and identified within this paper as being major issues. Agencies are advised to conduct an independent assessment to determine what other records management requirements may apply and seek independent legal advice should they wish to enter into contractual arrangements with a cloud vendor.

Executive Summary

This Issues paper was commissioned by the Public Record Office Victoria (PROV) to examine the recordkeeping implications of operating in a cloud computing environment. In that past two years the uptake of cloud services has increased dramatically and in last year, several federal government agencies, including the Australian Taxation Office (ATO) have adopted this approach. Cloud vendors have alluring offerings that no longer require agencies to maintain the burden of capital investment in hardware and infrastructure. Although the attraction of up-taking or entering into service agreements may present significant cost savings, Victorian government agencies need to undertake a thorough risk assessment in line with the Federal governments Protective Security Policy Framework (PSPF). Agencies should be aware that the move into cloud computing involves a risk based approach.

Victorian government agencies, regardless of the environment that records are stored in, must comply with the mandatory Standards and Specification issued by PROV. In a recent report into *Cloud Computing Security Consideration* undertaken by the Department of Defence, the Defence Signals Directorate (DSD) recommended against the outsourcing of information technology services and functions outside of Australia, unless agencies are dealing with data that is publically available. DSD encouraged agencies to choose either a locally owned vendor or a foreign owned vendor that is locally based and stores, process and manages data within Australian jurisdictions. PROV reiterates this recommendation throughout this document with regard to a recordkeeping context.

This issues paper offers PROV's stakeholders an opportunity to consider and comment on the following:

- Unauthorised access to classified information;
- Loss of access to data;
- Inability to ensure data integrity and authenticity; and
- Understanding the practical aspects of cloud services.

The issues paper also proposes recommendations to help Victorian government agencies in dealing with cloud vendors. In particular proposed recommendations are made in the following areas:

- Managing risks;
- Selecting a provider; and
- Contractual arrangements

The issues paper provides an opportunity for PROV to directly engage its stakeholder's who are considering, or who have made the transition to recordkeeping in a cloud environment. The comments and feedback received from the issues paper will result in PROV finalising its policy direction on the *Recordkeeping Implications of Cloud Computing Policy*.

Yours Sincerely

David Brown
Acting Director and Keeper of Public Records

1. Introduction

The Public Record Office Victoria (PROV) is the state record authority for Victoria. Established under the *Public Records Act 1973* (hereafter referred to as the Act), PROV's objectives are to:

- Issue mandatory Standards and Specifications regulating the creation, maintenance, security and disposal of public records;
- Advise and assist agencies in achieving compliance with issued standards;
- Preserve public records of permanent value as the State Archives; and
- Ensure that archives are accessible to the people and government of Victoria.

PROV has a duty in advising those required to comply with the Act (hereafter referred to as agencies) on appropriate management of records. The cloud computing policy will align with the recently revised Recordkeeping Standards issued by PROV. The purpose of this issues paper is to identify implementable solutions to the recordkeeping issues of cloud computing. The aim of the paper is to ensure that data is managed properly in a cloud computing environment.

Cloud computing is a means of enabling 'on-demand network access to a shared pool of configurable computing resources' that may be 'rapidly provisioned and released with minimal management effort or service provider interaction'[1]. Cloud computing is currently being used by Federal and State government organisations in Australia. It promises to offer significant cost savings by reducing the outlay of capital and investment in information technology, including software and hardware.

Benefits of using cloud computing lie in the opportunities for better agency service delivery including:

- Lower costs (capital equipment, operational costs, proprietary software);
- Scalable, self-service provisioning with no large upfront capital outlays. Customers are able to attain a 'custom fit'[2], as they can request services from the provider with relative ease;
- Reduced pressure on Information Technology (IT) teams to provide increased storage capacity;
- Redirection of resources as server maintenance and related IT tasks are reduced;
- Access to services available outside traditional office environments; and
- Adaptability (the flexibility of the cloud offers an IT based solution for almost any operating environment).

Broadly stated, potential risks of implementing a cloud system include:

- Unauthorised access to classified information;;
- Privacy breaches;
- Data alteration (either by unintentional data degradation, or by an unauthorised user); and
- Loss of access to data.

[1] P Mell & T Grance 2010, *The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Gaithersburg, viewed 22 November 2011, < http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>*

[2] "Custom Fit" refers to services that are tailored to an agency's needs.

1.1 Overview of the Recordkeeping Issues Paper on Cloud Computing

This issues paper will form the base of a *Recordkeeping Implications for Cloud Computing* (RICC) policy.

A RICC policy will:

- Establish an approach to records management in a cloud computing environment that is based on assessment of the risks;
- Identify recordkeeping risks and suggest practical solutions to mitigate identified risks;
- Provide direction on recordkeeping in the cloud environment that is in line with PROV Recordkeeping Standards;
- Make recommendations for agencies undertaking or proposing to undertake recordkeeping in the cloud environment.

1.2 Purpose of this issues paper

The purpose of the issues paper is to obtain feedback on cloud computing issues. This will assist PROV to identify solutions in a recordkeeping context and establish PROV's policy direction. Feedback may also ensure that solutions proposed by PROV are viable and practical. This Issues paper will:

- Set standards that are mandatory in Victorian government agencies;
- Define the issues;
- Identify practical solutions and make recommendations that will be detailed further in the RICC; and
- Invite stakeholder comment in order to become more aware of issues and solutions of relevance to Victorian government.

The constraints of the issues paper are as follows:

- Recommendations made will be in line with best recordkeeping practice;
- Issues will be based on risks to the secure capture, preservation, use and appropriate disposal of data; and
- Solutions will comply with the legislative requirements of the Victorian government jurisdiction.

1.3 Scope of the Issues paper

The issues paper explores the following recordkeeping risks and benefits from a transition to a cloud based infrastructure:

- Systems limitations (section 2.3);
- Managing risks (section 3.1);
- Selecting a provider (section 3.2);
- Limitations of vendors terms of service (section3.3);
- Contractual Arrangements (section 3.3);
- Unauthorised access to data (section 4.1);
- Loss of access to data (section 4.2);
- Difficulties in tracking and controlling data storage (section 4.3); and
- Understanding the practical aspects of cloud services (section 4.4).

Areas outside the scope of this document include:

- Cloud computing issues that are not directly relevant to recordkeeping;
- Technical aspects of setting up a cloud service;
- Cloud service delivery in lieu of onsite information technology investment; and
- Vendor business arrangements for adopting the cloud.

1.4 Responding to the issues paper

Please respond to those questions or aspects of the issues paper to which you may have particular views about. In your response please identify both the section of the issues paper and the questions, issues and paragraphs to which you are responding. Additional ideas or comments on matters not addressed in the issues paper are welcome. Please include them at the end of your response to a particular matter raised in the issues paper.

In responding to this issues paper agencies should be aware that PROV may be legally required to release the content and details of any response. If you have any concerns about information provided in your response, it is suggested that you seek legal advice.

Please email your responses to: Standards@prov.vic.gov.au

The closing date for responding to the issues paper is: **31 May 2012**

If you have any questions, pleases contact Christopher Wallace, Manager, Standards and Policy at Christopher.Wallace@prov.vic.gov.au or 03 9348 5720.

2. Cloud computing basics

In order to assess whether or not a cloud computing solution will address recordkeeping responsibilities, agencies will need to understand something about the technological environment within which the cloud operates. This includes understanding the software applications used by cloud service providers.

2.1 What is cloud computing?

The National Institute of Standards and Technology (NIST), a United States Department of Commerce agency, defines cloud computing as:

"*a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*[3]".

This definition is adopted by the Commonwealth Government of Australia. The characteristics of cloud computing as identified by NIST are described below:

- **On-demand self-service:** A user can access computing resources as required (such as server time or storage) with no or incidental service provider interaction.
- **Broad network access:** Resources are made available over the network and can be accessed through diverse media (for example, mobile phones, tablets, laptops and workstations).
- **Resource pooling:** 'The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model'[4], with resources dynamically provisioned based on demand.
- **Rapid elasticity:** Users can access computing capabilities as they require them, with resources scaling inward and outward to meet demand.
- **Measured Service:** Resources are controlled and optimised through a metering process. Resource usage can be monitored, controlled, and reported on, providing transparency for both the provider and consumer of the utilised service.

As the NIST definition is being widely accepted across Federal government, PROV is accepting this definition as applicable for Victorian government.

Question

Q 2.1-1: Is this definition of cloud computing still current in terms of your agency and are the characteristics still relevant?

Q 2.1-2: Does it apply to the recordkeeping aspect of cloud computing?

Q 2.1-3: If the definition was to be changed to match the needs of Victorian government, how would you define cloud computing?

[3] P Mell & T Grance 2010, *The NIST Definition of Cloud Computing, National Institute of Standards and Technology, Gaithersburg, viewed 22 November 2011, <* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf*>*

[4] Mell & Grance 2010 p. 2

2.2 Common recordkeeping characteristics of cloud computing

The following are characteristics that are shared by all forms of cloud computing, that have implications for recordkeeping:

- Victorian government information may be held outside direct government control;
- location may not be known to the agency or, if known, not accessible;
- Information may be held outside the Victorian or Australian jurisdiction;
- Infrastructure may be shared with other users; and
- The more difficulty in replacing the vendor offering, the higher the risk for agencies.

2.3 Categories of cloud computing

Various types of cloud environments may be provided by a service provider. Cloud services in most case fall under one or more of the following three categories:

- Software-as-a-Service (SaaS);
- Platform-as-a-Service (PaaS); and
- Infrastructure-as-a-Service (IaaS).

In essence, the cloud is delivered as a service to clientele encompassing either one or more of the three service models above. It is the service nature of the cloud that offers benefits to agencies. Cloud computing capabilities are rented and require no investment (short term or long term) in asset hardware or software[5].

Software-as-a-Service (SaaS)

Software-as-a-Service provides complete business applications delivered over the web.[6] The business applications are hosted by a provider and delivered as a service term (such as email or financial applications).

Applications are accessed from various devices through a client interface such as a web browser or through a program interface. The cloud infrastructure, including applications, servers, operating systems and storage, is managed by the provider.

Table 2.3.1 Controls within SaaS[7]

	Hardware	***Operating Systems***	***Support Environment***	***Applications***
Agency				
Vendor	√	√	√	√ (primary)

[5] Dr M Williams 2010, *New Tools for Business, A Quick Start Guide to Cloud Computing, Moving Your Business into the Cloud*.
[6] Williams 2010.
[7] Department of Defence 2011, Cloud Computing Security Considerations, p3

The benefits of Software-as-a-Service include:

- The ability to obtain software on a per-use basis, as there are no upfront costs from the service provider. However, upfront work is needed to load data or records into the application database and ongoing work is needed to integrate data and records between internal and external cloud data stores;
- Agencies can use common business applications without a requirement for in-house expertise in those applications;
- There is a reduction in agency capital expenditure almost immediately; and
- Agencies may test new software on a rental basis, with the option to continue to use and adopt software if it proves suitable.

Potential risks of Software-as-a-Service for an agency include the following:

- The vendor may not be receptive to altering service offering or contract to take into account Victorian requirements;
- Application software may be incompatible with agency recordkeeping systems resulting in hybrid systems that require a large amount of user intervention to ensure data is kept and managed appropriately;
- Lack of control over software, hardware, operating systems and applications make it difficult for legislative and regulatory compliance to be met;
- If the service is unavailable for lengthy periods the agency will be unable to continue operations until the service is restored; and
- Long-term preservation of data may be compromised if the service offered uses formats with a limited lifespan.

Many applications do not include recordkeeping functionality or considerations. This means that certain service and deployment models may not meet all of the records management requirements for compliance and regulatory demands under the Act. For example:

- Maintenance of the records integrity for their full lifecycle;
- Maintenance of links between records and their metadata; and
- Transfer of records (for example, to PROV as State Archives) or destruction of temporary records according to approved disposal authorities.

PROV considers SaaS to be a high risk model as the vendor has the majority of control over agency data. SaaS has a higher risk in that it is more difficult to replace the vendor offering.

Example

In late 2008 Guardian Media Group (GMG) began a switch from Lotus Notes e-mail and Microsoft Office applications to Google based applications. Within the first six months 300 Google sites had been set up for internal collaborations and 70 per cent of users had accessed their accounts. GMG adopted a system that would address their needs for a more productive and collaborative workplace. The decision to switch to SaaS and place their data in the public cloud was not taken lightly. GMG conducted a detailed risk assessment that addressed security concerns and potential security risks. There was also concern about the sensitivity of information being stored in the United States (US), where the *Patriot Act* allows the government to inspect any data stored on its shores. Google systems allowed Google full control of GMG's information, including setting access permission and deleting data.[8]

[8] Williams 2010.

***Note:* The US *Patriot Act* may not be as simple to overcome as illustrated in the example above. If agencies adopt a cloud service provider whose SaaS infrastructure is based in the US, then at some point agencies may be liable for privacy breaches if records and data are accessed under the *Patriot Act* (USA). Any organisation that has US ownership may be required to supply access to data under the Patriot Act, regardless of where the server concerned is actually located.**

In the recordkeeping context software-as-a-service is most beneficial when the software is a commodity, all email programs for example provide such functions. It is least beneficial where mature IT-based infrastructure and mission critical applications are in use. Software-as-a-Service almost inherently will require data to be maintained elsewhere.

Platform-as-a-Service (PaaS)

Platform-as-a-Service is the online delivery of a custom application development or deployment environments in which applications can be built and run on service provider systems. Developers can build custom web applications without installing any tools on agency computers and then, deploy those applications without requiring specialised system administration skills. The infrastructure required is supplied by the cloud service provider. The agency has control over the deployed applications and possibly the configuration settings for the environment.

Table 2.3.2 Controls within PaaS[9]

	Hardware	***Operating Systems***	***Support Environment***	***Applications***
Agency				√ (operating environment)
Vendor	√	√	√	

Benefits of Platform-as-a-Service include the ability for an agency to:

- Redirect finances from infrastructure to the creation of applications;
- Take advantage of easy-to-use processes for developing, maintaining and deploying applications; and
- Not to acquire specialised expertise in website development (such as server development or website administration).

Potential risks of Platform-as-a-Service for the agency include the following:

- Business applications may not be portable as they are built in the vendor's environment, and moving to another cloud vendor if required, may be difficult;
- Contracts may lock the agency into using the one vendor for all services, limiting the agency's ability to take advantage of software or applications that are more suited to the agency's needs;
- If circumstances change, the agency may not be able to adjust the service provided to suit – for example, new legislation may require services that the cloud provider can not accommodate; and
- Setting up a service that meets the needs of the agency can be expensive.

PROV considers PaaS to be a high risk model as there is a high risk of locking agency applications to vendor environment, which means data is locked to vendor's servers.

[9] Department of Defence 2011, p3

Example

Menumate is a provider of point-of-sale hardware and software for the hospitality industry across Australasia. Menumate has taken advantage of PaaS to migrate over time a series of legacy applications used in business. The PaaS infrastructure has allowed Menumate to centralise, modernize and integrate an in house software toolkit. Connectivity and security issues are inherently provided. Using a PaaS approach has meant that Menumate can take advantage of both existing integrations and automated deployment tools, creating customer records which are integral to the business[10].

Infrastructure-as-a-Service (IaaS):

Infrastructure-as-a-Service is the online delivery of virtual infrastructure components (such as servers, storage and network access). It provides consumers with generic computing resources, such as the infrastructure needed for users to deploy and run their own software applications. IaaS can be seen in the development of the Internet Service Provider (ISP) model, where service providers rent infrastructure for the purpose of running applications instead of buying and installing them in their own data centre.

Table 2.3.3 Controls within IaaS[11]

	Hardware	***Operating Systems***	***Support Environment***	***Applications***
Agency			√	√
Vendor	√	√		

Benefits of utilising IaaS include:

- Agency provides application and support environment, allowing the agency the opportunity to build in its requirements;
- The ability to migrate easily from vendor to vendor;
- Agencies can control what computer resources are used and how they are used, making it easier to comply with legislative and regulatory requirements;
- When seeking compatibility with agency recordkeeping systems as it may be possible to configure systems and applications to enable integration; and
- Agencies can manage data preservation so that information is retained for the duration it is required to be kept.

Potential risks of Infrastructure-as-a-Service for the agency include:

- Multiple organisations may be using the same infrastructure; there is a possibility for data security to be breached.

PROV considers IaaS to be the model most commonly used across Victorian government. As the majority of control rests with the agency rather than the vendor, it is considered to be relatively low risk. Care should be taken to prevent others using the same service from accidentally gaining access to the agency's data.

[10] Williams 2010.
[11] Department of Defence 2011 p2

Example

In November 2007 Derek Gottfrid, a developer from the New York Times used Amazon Web Services (an IaaS environment) and technical skill to solve a difficult problem for his employers. The newspaper wanted to make all its public domain articles from 1851-1922 available on the web free of charge, but the articles were broken up into individual images scanned from the original paper that had to be pieced together. This could be done on a website but if the website proved popular then the web server could be overloaded with processes and grind to a halt. There were 11 million articles to process and a tight deadline to meet. Gottfrid's solution was to use open source tools to process the four terabytes of image data on 100 Amazon virtual machines (IaaS). The whole process took 24 hours and cost USD $240.

Question

Q 2.3-1: Is the use of services offered by the cloud likely to relieve your agency's IT management burden and enhance your business?

Q 2.3-2 Is the use of services offered by the cloud likely to create complex and new issues in your IT management?

Q 2.3-3 Are there any other cloud services being offered that have not been identified?

2.3.1.1 Cloud Deployment Models

Cloud computing is provided in the following deployment models:

- Private Cloud;
- Public Cloud; and
- Community Cloud

Initially cloud referred to software accessed over the internet[12]. It was quickly realised that cloud environments could be setup internally as well as externally, which lead to the development of three broad deployment models.

Private Cloud: The cloud infrastructure is provisioned for exclusive use by a single organisation (such as an agency) comprising of multiple consumers (such as various business units). It may be owned, managed and operated by the agency, a third party, or a combination of both, and it may exist on or off premises.[13]. The private cloud gives an organisation more control over their Information and Communication Technology (ICT) environment by offering increased privacy and security for data. The private cloud deployment model can be broken down into:

- Private Cloud: in house: uses cloud technology to provide flexibility but retains security.
- Private Cloud: service provider: the private cloud is provided by a service provider. In theory this retains security but have to check what is really provided.

[12] Oracle White Paper (2009), *Platform as a Service, Private Cloud with Oracle Fusion Middleware*.
[13] NIST, p.3.

The Private cloud deployment model can be recognised by the characteristic that the resources are only used by the agency. This means that the risk of unauthorised access is reduced. A private cloud deployment model could be provided by a third party over the internet. In such cases, the differences between private and public clouds can be difficult to distinguish as it is not clear what resources are shared.

Benefits of a private cloud include the ability for an agency to:

- Provide IT services to internal users in a self service manner;
- Automate management tasks (software and desktop updates), and individually bill business units for services consumed;
- Enable a well-managed business specific ICT environment; and
- Optimise the use of agency resources, including servers.

Potential risks in using a private cloud deployment model for an agency include the following:

- The level of technical skill required for the agency to implement and operate a private cloud may be greater than anticipated and result in the need to provide additional resources to maintain; and
- The costs required to set up and operate a private cloud may be larger than the available or anticipated budget.

Service providers may offer the capacity to set up either a private or public cloud environment. In many situations the services provided are very similar. Care should be taken to ensure that in a private cloud it is the agency that holds, and has full control over, its data and the systems within which it operates.

Public Cloud: Services delivered using a pool of shared resources to any organisation over a public internet connection. Public clouds are likely to be cheaper than private clouds to use. The distinction between a public and a private cloud may not be clear if a private cloud is run by a third party as their characteristics and risks will be very similar. The risk is linked to who is holding the data.

Benefits of a public cloud include the ability for an agency to:

- Scale the cloud environment to agency's business needs;
- Pay for deployment as it is used;
- Access a larger pool of resources;
- Shared joint costs across public cloud users; and
- Ensure certainty that the cloud services are available and reliable.

Potential risks in using a public cloud deployment model for an agency include the following:

- As multiple organisations use the same infrastructure, there is a possibility for data security to be breached; and
- Contracts may lock the agency into using the one vendor for all services, limiting the agency's ability to take advantage of software or applications that are more suited to the agency's needs.

Community Cloud: The cloud infrastructure is shared by more than one group in a specific community (such as CenITex, or a group of agencies with similar operating, security and compliance considerations). The goal of a community cloud is to have participating organisations realise the benefits of a public cloud, multi-tenancy and a pay-as-you-go billing structure but with the added level of privacy, security and policy compliance usually associated with a private cloud. It may be managed by those using the cloud service or a third party. Infrastructure may exist remotely or on the premises of one or more agencies.

Benefits of a community cloud include the ability for an agency to:

- Reduce IT costs and resources due to their being shared between agencies; and

- Increase security of information services as the need for external interaction with agency data is reduced.

Potential risks in using a community cloud deployment model for an agency include the following:

- Meeting privacy requirements may require an additional level of security across centralised systems that reduce their usefulness as shared resources; and
- Not all computing needs may be met as an agency may find some computing resource needs to be specialised and not required by other agencies in the community.

A fourth deployment model, the **Hybrid Cloud** consisting of a combination of the above three models, may also be used. Benefits and risks concerned will match those of the specific deployment models used to create the hybrid cloud.

A comparison of private and public cloud environments

The main difference between a private and public cloud is control over the environment. In a private cloud, the agency (or a trusted partner) controls the service management agreements, whereas in a public cloud these agreements are controlled by the service provider. Be sure that the deployment model offered is what it appears to be and not a marketing ploy whereby a vendor offers differently priced packages of the same services.

Both the public and private clouds in theory offer the following benefits to the agency:

- Efficiency;
- High availability; and
- Elastic capacity.

In addition to the above benefits, public clouds offer the following to an agency:

- Lower upfront cost;
- No hardware investment for setup of infrastructure or services; and
- Minimal systems management by the user.

Public clouds have risks that an agency should be aware of, including the following:

- Potentially more difficult in integrating with agency systems;
- Difficult integration constraints depending on your recordkeeping system; and
- Loss of control over security and quality of systems in which data is held.

Private clouds require minimal investment in hardware when compared to full IT based infrastructure as well as setup and ongoing maintenance. The benefits of maintaining records in a private cloud could potentially reduce the risks that may be experienced in a public environment. At a minimum private clouds offer:

- Greater control of data over time;
- Full access and flexibility to integrate with agency EDRMS; and
- Direct control over quality and security.

Recommendation 1: As private clouds and community clouds offer less risk for higher risk records, agencies should deploy either the private or community cloud model.

Question

Q 2.3-4: Which service and deployment model is most appropriate for your agency's needs?

Q 2.3-5: Why does the agency consider the service and deployment models identified at Q2.2-4 to be the most appropriate?

3. Vendor Issues

Unless the vendor is the agency or Victorian Government, a third party will be needed provide cloud services.

It is the responsibility of the agency to ensure that the service provider can adequately look after the records and the system they are stored in. The best way to determine what recordkeeping risks may be involved with implementing a cloud computing solution is to conduct a thorough risk assessment prior to engaging a third party. Key risks include the breach of legislative requirements, such as those imposed by the Act, the *Information Privacy Act 2000*, the *Freedom of Information Act 1982* (FOI), the *Evidence Act 2008*, and the *Crimes Act 1958*. They also include loss of valuable business information, as well as the possibility of embarrassment or even placing people's lives in danger due to the inappropriate release of information in extreme cases.

Recommendation 2: Agencies should conduct a thorough risk assessment prior to adopting a cloud computing environment and consider risk mitigation strategies, as some data may be so sensitive that it should never be stored in a cloud. Agencies should be familiar with the Protective Security Policy Framework (PSPF).

3.1 Managing Risk

The Standards and Specifications issued by PROV are mandatory. Regardless of the jurisdiction in which the records are held, agencies may be held accountable against PROV's Standards and Specifications by regulatory authorities, including the Victorian Ombudsman and Victorian Auditor General's Office. Agencies need to ensure that the evidential nature of records will not be compromised.

Managing risk should include the following actions:

- Identify the records to be stored and processed using cloud service providers;
- If possible attend the location of the services to ensure adequate measures are in place (including disaster preparation, management and recovery);
- Ensure 'due diligence' is performed when selecting a provider;
- Manage identified risks through contractual arrangements; and
- Monitor cloud computing services offered by the provider.

Recommendation 3: Agencies should ensure that vendors are able to demonstrate and exhibit due diligence (a thorough investigation or audit of the cloud service provider, prior to signing the contract).

3.2 Selecting a provider

When performing due diligence checks, Agencies are advised to consider the questions and key actions identified in Table 3.2.1 (below).

469 Table 3.2.1 Questions and key Actions to Consider when selecting a service provider

Question	***Key Actions***
Where will the records be stored?	- Determine the processes around reporting storage location changes to the agency.
Can the cloud service provider meet the requirements of the PROV Recordkeeping Standards?	- Provide vendors with copies of the PROV Recordkeeping Standards. - Include in the contract or agreement a requirement to meet PROV Standards.
Is the service provider aware of the requirements of the *Information Privacy Act 2001*?	- Establish the level of compliance with the IPA privacy principles. - Determine the jurisdictional legislation that the records may be subjected to.
Will all records be returned to the agency, by the service provider within an agreed timeframe once the contract has ended?	- Establish the processes involved in completely returning a copy of agency specific data. - Establish the process for completely erasing the data from the vendors system. - Include in the contract any costs involved in removal of data.
What assurance can the provider supply to the agency that no copy of agency data has been retained after the termination of the contract?	- Determine effective 'take down' procedures for potential compliance breaches. - Verify vendor certification of the total and permanent removal of the requested records from the provider's systems (including back up copies).
Is the service provider subject to external auditing, certification or monitoring processes?	- Determine whether vendors are subject to external auditing or certification processes. - Establish whether the external monitoring is sufficient to mitigate or reduce data access or storage risks.
How will third party access to the agency's records be managed by the service provider?	- Determine how Freedom of Information (FOI) requests of agency records can be effectively managed. - Identify provisions for third party access to data stored in non-Australian jurisdictions.
What back-up arrangements does the service provider have in place to ensure the restoration of agency data?	- Obtain vendor guarantee that the structure of agency records and associated metadata are maintained when restoring data. - Verify back-up arrangements are in place, how long it would take to do a complete restoration of agency records, and any additional costs. -Testing.
What risk assessments does the cloud service provider conduct in relation to the storages of an agency's records.	- Establish if the provider guarantees service provision parameters and levels of liability for failure to operate within the given parameter. - Direct vendor to conduct risk assessment of storages of an agency's records.
What subcontracting arrangements does the service provider undertake?	- Ensure the agency will be notified of any subcontractor access to agency records (including what level). - Determine the extent the vendor subcontracts services and the impact this may have on agency data.

3.3 Contractual Arrangements

Where computing resources are provided as a service, much of the relationship between the agency and the provider will be governed by a contract. This will require both:

- IT contract negotiation skills to establish the terms of the relationship; and
- Records management knowledge to ensure that recordkeeping requirements regarding management of data are adequately met.

Contracts or agreements with service providers based or owned outside of Australia can be problematic to enforce. Even if an agency is able to take the service provider to court over a breach of contract, it is likely to be difficult to enforce their findings on an overseas vendor. Furthermore agencies should recognise that they may have little leverage over vendors.

Service Level Agreements

Service level agreements (SLAs) should be included in the contract to outline specific parameters and minimum levels for each aspect of the service provided. SLAs must be enforceable and specify remedial actions for when they are not met, including corrections and penalties.

Examples of measurable services that may need to be covered in an SLA include:

- Uptime, the availability of service and who determines whether the service level was met;
- Performance and response time, including the speed of the service;
- Capacity and efficiency (non speed related) of the service;
- Error correction, maintenance time and the availability of a help desk. A root cause analysis should be supplied by the service provider after any service failure;
- Compensation and the right to terminate the SLA;
- Restoration of the data; and
- Maximum time for return of all data in a usable form.

PROV Requirements and Contracts

Ensuring appropriate records management clauses in contracts with cloud computing service providers can assist in meeting the requirements relating to outsourced activities and privatisation in the PROV *Strategic Management Specification*. For agencies to meet the requirements of the *PROS 10/10 S1 Strategic Management Specification* when engaging a cloud service provider, agencies must ensure the contract covers:

- The ownership and custody of records is determined and documented (see Requirement 21);
- The service provider must be required to comply with records management requirements determined by the agency (see Requirement 22);
- Records must only be disposed of in accordance with the Act and other relevant legislation (see Requirement 23);
- The same level of access to records must be available to the public, regardless of who is delivering or provisioning the service (see Requirement 24);
- To specify appropriate standards of storage for any records of outsourced or privatised activities which are not in government custody (see Requirement 25);
- To specify appropriate standards of security for any records of outsourced or privatised activities which are not in government custody (see Requirement 26);
- Arrangements for monitoring and audit of service provider records management practices agreed and specified (see Requirement 27);
- All outstanding records management issues (including disposal) must be addressed by the service provider prior to the completion of the contract (see Requirement 28);and

- The total budget for the contract includes sufficient resources to fund the cost of the specified recordkeeping requirements (see Requirement 29).

Recommendation 4: Agencies must ensure that outsourced contracts or agreements with cloud service providers meet requirements 21 to 29 of *PROS 10/10 S1 Strategic Management Specification.*

Agencies must ensure that any contractual arrangements and service level agreements address the relevant recordkeeping requirements identified in PROV's Recordkeeping Standards and Specifications. More information about how the Standards and Specifications relate to cloud computing is provided in Section 5.

Data Processing and Storage

As the agency's data will reside on the service provider's infrastructure, it is important for the agency to affirm its ownership of that data in contracts or agreements. It may also be necessary for evidential and business purposes to affirm agency ownership of any transactional data created as a result of data being processed on the cloud computing provider's system.

The agency should establish itself within the contract as the controller and determine the purpose and means of processing data. The cloud service provider's role within the contract should be defined as the processor, processing data on behalf of the controller[14].

The contract should nullify "vendor lock in" (locked into a particular vendor's cloud). The agency must have the right to change to a different offering when a contract ends. The agency may want to move data back in-house or to a new vendor. Compatibility and interoperability of data should be ensured after the termination of contractual agreements.

The agency's ongoing rights to access its data and the process by which data will be migrated back to the agency should be stated within the contract. It should outline the timeframe within which the vendor needs to return data and specify the format of the data.

The service provider's obligations in the event of unauthorised access of agency data must be covered within the contract. This includes the requirement to notify the agency of any data breaches, the timeframe for notification and the disclosure of breach details. It also includes provision of compensation if the agency's data is accessed inappropriately.

Due to the range of legal and regulatory issues that can arise if data is stored in another state or country, it is important to specify and document the geographic location of the data centre. Any proposed changes to the data storage arrangements should be approved by the agency. This is particularly important when records are stored and transmitted outside of Australia.

Infrastructure and Security

The cloud provider's security measures should be clearly documented in the contract, including specific infrastructure and security requirements and practices. This may include business continuity, disaster recovery, firewalls and physical security.

A right-to-audit contract clause should state requirements for third party audits or certifications and the provision of any reports generated from these activities to the agency.

---

[14] Dr M Williams 2010, New Tools for Business, A Quick Start Guide to Cloud Computing, Moving Your Business into the Cloud,

Vendor's infrastructure and security practices would ideally be confirmed via on-site inspection. Alternatively the agency could obtain the provider's infrastructure and security specifications in writing and have in-house experts review and confirm their suitability. An agency must have the right to break the contract if a vendor does not meet the contractual obligations as a result of subsequent changes to their service delivery.

Cloud computing services could be disrupted by disasters or other unforseen circumstances. The contract should state the provider's disaster recovery procedures and business continuity plans to ensure the agency has ongoing access to its data. The contract should also outline the service provider's obligations if any of the agency's data becomes lost or damaged due to vendor error. It should outline the notification process, corrective actions to be taken, timeframes, plans for ongoing service provision and the vendor's obligation to reimburse costs.

Vendor Relationship

Establish the terms under which the agency can continue to use the service as well as those under which it can make changes or terminate the service. This can help to avoid large costs associate with changing to another solution.

It may be necessary to negotiate the costs for expansion of volume or usage. One of the major benefits of cloud computing is scalability. It is important to ensure the contract doesn't specify minimum purchase volumes or long-term commitments.

Cloud computing is a constantly evolving field where features and functionality can be added and removed. It may be pertinent to include a requirement for notice to be given to the agency prior to the removal of a feature or functionality or the cloud computing service. The notification period should take into account the time it would take for the agency to move to a new solution.

The contract should detail terms under which the agreement can be terminated either by the agency or the vendor. Considerations for the agency would be whether cause would have to be shown or fees or penalties incurred. Agencies may wish to negotiate a clause that restricts the vendor's right to terminate the service. This could include a suitable period of advance notice.

Mergers and acquisitions present risks to the ownership of data and the maintenance of data integrity and ongoing access to that data by the agency. Agencies must ensure that *break clauses* in the contract provide the agency with an opportunity to break the contract.

It is common for cloud computing providers to subcontract services to third parties, for example, vendors may subcontract the data centre infrastructure. This has the potential to create confusion over which vendor is responsible for which actions. The contract should oblige the vendor to identify any functionality that is being outsourced and to whom. It should be made clear that the contracted provider remains directly responsible for complying with the terms of their contract irrespective of subcontracting.

Question

Q 3.3-1: Is your agency subject to regulatory compliance or internal governance restrictions?

Q 3.3-2: If so what are they?

Q 3.3-3: Do they prevent your agency form using a cloud service provider?

4. Recordkeeping issues of cloud computing

Agencies seeking to implement cloud computing services are advised to consider the implications for their records management program. It is the agency's responsibility to ensure that data stored in a cloud complies with Victorian legislation and regulations. This means having clearly assigned and documented lines of authority and accountability with regard to the data stored in a cloud environment. Personnel, including contractors and volunteers, must be made aware of what needs to be done to ensure that the agency's recordkeeping responsibilities are met.

Recordkeeping responsibilities are identified in legislation, regulations, policies and Standards (including PROV's Recordkeeping Standards). Agency data stored or created in any cloud are subject to the same records management standards and obligations as agency data stored in other environments within the State of Victoria. Agencies must ensure that they are compliant with PROV's mandatory Standards and specifications.

An element of strategic planning is required to ensure that different sections of the agency are aligned. Key areas include information technology, records management, risk management and contract management. This will ensure that risks are identified and mitigated as part of the agency's risk management framework and that contracts include clauses related to the various recordkeeping responsibilities the service provider is to meet. PROV also recommends that agencies familiarise themselves with the Commonwealth Government's, Department of Defence Intelligence and Security discussion paper on Cloud Computing Security Considerations. Agencies must be aware must be of the sensitivity of the data they are proposing to store in the cloud environment. Risks will vary depending on the sensitivity of this data[15].

As cloud computing will most likely be offered as a service by a third party, recordkeeping responsibilities will need to be managed through a contract or agreement to meet the principles of *PROS 10/10 Strategic Management*. Section 2.4 of the associated Specification (PROS 10/10 S1) identifies the recordkeeping requirements that contract clauses will need to cover. *Strategic Management Guideline 2: Managing Records of Outsourced Activity* provides some sample clauses that may be useful when considered clauses to manage cloud computing risk.

This section of the issues paper explores some of the significant recordkeeping implications for agencies choosing to adopt a cloud computing model. There will be other issues, both general and unique, to a particular agency that are not discussed in this paper.

4.1 Unauthorised Access to Data

The first recordkeeping issue with cloud computing is the prevention of unauthorised access to data stored in a cloud server. Unauthorised access could be by:

- Eavesdropping on the network traffic between the agency and the cloud server;
- Staff at the cloud service supplier using administrative tools to obtain data. This could be for personal purposes, or required by local laws (e.g. the US Patriot Act);
- Other users of the shared cloud server deliberately or inadvertently accessing agency data;

[15] Australian Government, Department of Defence (2011) Cloud Computing Security Considerations

- Outsiders breaking the service provider's security. These outsiders could be individuals, organisations, or governments. Outsiders could be extremely well resourced and knowledgeable; and
- Leakage of data from decommissioned media.

It is the agency's responsibility to ensure that the service provider implements adequate security measures to protect their data, in particular agencies must consider the risks associated with handing over control of records to external vendors.

The level of security measures required will depend on the sensitivity of the data. Data that is publically available will need little or no security measures. Data that is sensitive or personal will require substantial security measures. Security related data will require very substantial security measures, and it is likely that this type of data would not be appropriate for storage in a public or community cloud.

Security requirements for private clouds operated in-house will not be considered in this document, as the security would be little different to that required by any web accessible agency system.

When identifying security measures for cloud computing solutions, the following constraints must be met:

- Compliance with the *Information Privacy Act 2000* (Victoria).
- The Protective Security Policy Framework (PSPF) provisions may also need to be complied with.
- PROV Storage Standard Principle 6 that public records must be protected from theft, misuse, and inappropriate or unauthorised access or modification, while they are being stored, or in transit to or from a storage facility or area.
- PROV Access Standard Principle 4 that public records must only be used for authorised purposes; taking into account all relevant legislation, access, copyright or licensing conditions.
- PROV Access Standard Principle 5 that the security of public records must be assured, preventing unauthorised access, alteration, destruction or release of records.
- PROV Disposal Standard Principle 1: Disposal of public records must be conducted in a lawful manner.
- PROV Disposal Standard Principle 8: The destruction of public records in accordance with a disposal authority must be undertaken using a secure method to ensure the content of the records is not released inadvertently.

Privacy

Regardless of where agency data is stored, it is subject to the *Information Privacy Act 2000* (Vic) (IPA).

Example

> Data stored in overseas jurisdictions may be subject to that jurisdiction's privacy laws (which may differ considerably from privacy data protection laws within Victoria). For example, the US Patriot Act and its associated anti-terrorism legislation permit the US government to access data under specified circumstances without providing any notification. This is likely to breach the Information Privacy Act 2000 (IPA); in particular the requirement of IPP 4, to protect personal information from unauthorised access. Information Privacy Principle 9 prevents the transfer of personal information outside Victoria unless the recipient protects privacy under standards similar to Victoria's IPPs. Many countries do not have legislation governing the protection and management of personal information.

The IPA sets a standard for the protection of the privacy of personal[16] information held by the State and local Government of Victoria. The IPA only applies to data that contains personal information about, or that can be used to identify, any individual. Agencies must ensure that contracted service providers have procedures in place to comply with the Information Privacy Principles (IPPs) that form the core of the IPA. Contractor and service provider agreements must enforce contracted providers to abide by the IPPs[17].

Security

It is the agency's responsibility to ensure that the service provider implements adequate security measures to protect their data.

Clearly the level of security measures required will depend on the sensitivity of the data. Data that is publically available will need little or no security measures. Data that is sensitive or personal will require substantial security measures. Security related data will require very substantial security measures, and it is likely that this type of data would not be appropriate for storage in a public or community cloud at all.

Security requirements for private clouds operated in-house will not be considered in this document, as the security would be little different to that required by any web accessible agency system.

It is understood that the Victorian government will move to adopt the *Commonwealth Government's Protective Security Policy Framework* (PSPF). PROV considers this framework to be good practice in analysing what data can be held outside control of an agency.

The PSPF identifies a number of mandatory requirements regarding developing and implementing a security plan. For example, the application of a security classification to all

---

[16] The *Information Privacy Act 2000* defines 'personal information' as 'information or an opinion (including information or an opinion forming part of a database) that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the *Health Records Act 2001* applies.

[17] http://www.privacy.vic.gov.au/privacy/web2.nsf/files/dont-let-privacy-get-lost-in-the-cloud/$file/media_release_03_05_11.pdf

data is required. Only those who have security clearance for a particular security classification may see the associated data. It is the agency's responsibility to ensure that contractors and service providers abide by the requirements of PSPF. Commonwealth agencies are currently required to provide the results of an assessment against the PSPF requirements in their annual report.

An area that may inadvertently lead to security breaches is the disposal of media on which data is stored. Service providers may routinely dispose of back up tapes and decommissioned systems and discs that contain agency data without removing the data prior to destruction or ensuring that the total destruction of the data has been achieved. Total removal of agency data from the service provider's systems may not be possible.

Disposal of data includes disposal of back up tapes and decommissioned discs that contain the data. To be lawful, disposal must be conducted in accordance with a PROV Disposal Authority. Some data will need to be transferred to PROV once it has reached its retention period. This should be done by the agency in accordance with PROV processes. Some data should be destroyed once the retention period has ended.

Decisions to destroy agency data in a cloud environment, including destruction of back up tapes and decommissioned disks, must only occur after consideration of the facts involved. This includes the disposal class and sentence relating to the data, the person authorised to approve disposal actions, and approved methods of disposal. The disposal class and sentence provide information on how long the data will need to be retained prior to its disposal and whether the data is to be destroyed or transferred to PROV.

Copies of data (such as those on back up tapes or decommission discs once the data has been migrated to other systems) may be destroyed under normal administrative practice (NAP). A record of destroyed data must be kept that includes the disposal authority under which the data was destroyed. This record does not include destruction under NAP.

Destruction of data, if it occurs, should be complete so that no reconstruction is possible. This includes destruction of back up tapes and decommissioned discs containing agency data. Secure destruction is needed to prevent private information from being accidentally released through inappropriate disposal methods. If the data being destroyed has restricted access due to a security classification assigned under the PSPF, the destruction may need to be witnessed by an authorised representative.

The capacity, and appropriate procedures and systems, required for disposal actions to be implemented include the following:

- Retention of data that is retrievable and understandable for the duration of its lifecycle;
- Transfer of data into the custody of another agency if required (for example, if a machinery of government change requires data relating to a specific function to be transferred to a different agency);
- Permanent value records transferred to Public Record Office Victoria; and
- Destruction of time-expired data (including any copies of the data) in a manner that ensures that the data is not be able to be reconstructed.

Regardless of where it is stored, agency data is subject to the PROV recordkeeping standards. These standards include requirements covering the security of agency data. Agency data may also soon be subject to the requirements of PSPF, regardless of where it is stored.

Cloud computing services must be able to ensure that the data is protected from theft, misuse, and inappropriate access or modification whilst they are being stored as well as when they are in transit to or from the storage facility or area. For cloud computing services,

this means that the online interface between the server and the agency must protect the data from unauthorised access as well as the systems used to store the data. Where data is subject to security classifications (such as the protective security policy or its equivalent) the level of protection required for the security classification must be ensured by the cloud service provider. Protection from hacking and unauthorised release of restricted data will also need to be ensured.

Under *PROS 11/10 Access Standard*, if data stored in a cloud environment has an access status of open, the level of protection required for the data is minimised. This is because anyone is allowed to view and use the data.

Where data has restrictions to access, the agency must ensure that the access restrictions are applied in the cloud environment. The level of support needed to administer the cloud services provided should be considered, including who will be providing the support and what data they will be able to access.

Questions

Q 4.1-1: Are there any other data access concerns that have not been identified in this paper?

Q 4.1-2: Are there any other constraints on solutions other than those identified in this paper?

Recommendations

Recommendation 5: PROV is proposing to require all agencies storing data on a cloud server to categorise the sensitivity of the data.

This analysis must consider:

- Whether the data is personal information as defined in the IPA; and
- The level of security required under the PSPF.

The risk analysis must be signed off by a senior business owner.

Security classification of agency data is already covered by the Capture, Storage and Access Standards, and includes the following:

- Records that carry security classifications are created and captured in compliance with the requirements of that classification (Capture Specification 3, Requirement 17).
- Records that carry security classifications are handled and stored in compliance with the requirements of the classification (Storage Specification 1, Requirement 37).
- Policies governing access to records align with legislation and Victorian government policy (Access Specification 1, Requirement 2).
- Documented criteria, based on legislation and policy, are used to justify restrictions on records (Access Specification 1, Requirement 5).
- Access restrictions for records are implemented in all appropriate systems (Access Specification 1, Requirement 6).
- Security measures, procedures and protocols relating to access to records are established, documented, and designed to prevent unauthorised access, alteration, destruction or release (Access Specification 1, Requirement 14).

The above recommendation is an extension of the existing requirements and would be covered in a Guideline on how to implement the Standards in a cloud computing environment. The Guideline would fit under Storage.

Questions

Q 4.1-3: Would there be any problem in implementing this recommendation in your agency?

Q 4.1-4: Are there any other criteria that should be considered in performing a sensitivity analysis?

Recommendation 6: PROV is proposing to recommend that agencies storing personal or sensitive data on a cloud server use servers located in an Australian jurisdiction. The company that operates the server must be registered in an Australian jurisdiction, although it may be a subsidiary of an overseas company.

Choosing a provider who delivers a service from within Australia would ensure that most privacy risks associated with recordkeeping are mitigated. This is due to the similarity of privacy legislation across the different Australian jurisdictions. A service provider based in Victoria is the preferred option due to other PROV recordkeeping requirements.

PROV would caution agencies seeking cloud service providers based offshore and would recommend that a comprehensive risk assessment is conducted. Using cloud computing services will impact on the degree of control an agency has over the way its data is managed and accessed by third parties. It may not be possible to adequately protect personal information stored outside of Australia. If data is stored offshore it could be difficult to enforce and monitor access and security provisions.

Third party storage of agency data is currently covered by the Storage Standard, and includes the following:

- Any commercially operated storage areas and facilities which store public records have been assessed as being compliant with this Specification by the Keeper of Public Records under the Approved Public Record Office Storage Supplier (APROSS) programme, and any conditions or limitations have been noted in the certification (Storage Specification 1, Requirement 3).
- APROSS storage areas and facilities have been inspected and assessed for compliance with this Specification by an APROSS representative and a report of compliance has been attested by the head of the APROSS annually and submitted to the Keeper of Public Records (Storage Specification 1, Requirement 7).
- The location of each storage area or facility has been subjected to a risk assessment to identify and mitigate possible risks to the preservation of and access to the public records stored there, and the results have demonstrated that the level of risk is low (Storage Specification 1, Requirement 10).
- Storage Specification 1 Requirement 11: Storage facilities have been assessed as being compliant with the Building Code of Australia and associated codes (Storage Specification 1, Requirement 11).

The above recommendation would require amendment of the PROV APROSS Programme to enable assessment of Australian storage facilities and areas outside of Victoria.

Questions

Q 4.1-5: Would recommending the use of a server located in an Australian jurisdiction unreasonably limit the use of cloud services, or unreasonably increase the cost?

Q 4.1-6: Would recommending the use of a company registered in an Australian jurisdiction unreasonably limit the use of cloud services, or unreasonably increase the cost?

Recommendations

Recommendation 7: PROV is proposing to recommend that, where agencies store data on a cloud server located outside an Australian jurisdiction, the agency has ensured that:

- The circumstances have been assessed by a Victorian legal expert on behalf of the agency with a documented recommendation from the legal expert that it is acceptable for the agency to store its data outside an Australian jurisdiction.
- The contract with the service provider follows industry best practice regarding records management in accordance with the legislative and regulatory requirements for the Victorian jurisdiction;
- Data is easily migrated to the agency or another service provider; and
- The provider will provide compensation for any breaches in privacy and make the necessary changes to its systems to ensure that the breach does not reoccur.

In executing a contract with a company registered outside an Australian jurisdiction, agencies should consider that

- Once data has been leaked the damage has been done. Any compensation will not repair the damage, or retrieve the data.
- It is likely to be extremely difficult to enforce any judgement.

Third party storage of agency data is currently covered by the Storage Standard, and includes the following:

- Any commercially operated storage areas and facilities which store public records have been assessed as being compliant with this Specification by the Keeper of Public Records under the Approved Public Record Office Storage Supplier (APROSS) programme, and any conditions or limitations have been noted in the certification (Storage Specification 1, Requirement 3).
- APROSS storage areas and facilities have been inspected and assessed for compliance with this Specification by an APROSS representative and a report of compliance has been attested by the head of the APROSS annually and submitted to the Keeper of Public Records (Storage Specification 1, Requirement 7).
- The location of each storage area or facility has been subjected to a risk assessment to identify and mitigate possible risks to the preservation of and access to the public records stored there, and the results have demonstrated that the level of risk is low (Storage Specification 1, Requirement 10).
- Storage Specification 1 Requirement 11: Storage facilities have been assessed as being compliant with the Building Code of Australia and associated codes (Storage Specification 1, Requirement 11).

Implementing recommendation 7 would require amendment of the PROV APROSS Programme to enable attestation by Victorian legal experts that overseas storage facilities and areas are compliant with Victorian jurisdictional requirements.

Questions

Q 4.1-7: Does this recommendation satisfy data protection and Victorian industry compliance requirements?

Q 4.1-8: Would there be any problem in implementing this recommendation in your agency?

Q 4.1-9: Are there any specific criteria that agencies should build into contracts with vendors outside Australian jurisdiction?

Recommendations

Recommendation 8: PROV is proposing to recommend that where personal or sensitive data is stored in a public or community cloud, a Protective Security Policy Framework analysis be performed.

Questions

Q 4.1-10: Would there be any problem in implementing this recommendation in your agency?

4.2 Loss of Access to Data

The second recordkeeping issue with cloud computing is the prevention of loss of access to data stored in a cloud server. Loss of access could be by:

- Scheduled or unscheduled network shutdown periods;
- Vendor bankruptcy or sale to new service provider;
- A disaster that destroys the vendor's systems; and
- Hackers or other internet criminal activity.

The use of cloud computing services relies on access to the internet and the continuity of access to data and applications. Agency data contain evidence of citizen entitlements, enable business continuity, assist with investigations, and enable an understanding of history. Prolonged loss of agency data may have severe consequences in one of these areas.

Cloud computing issues related to the loss of access to data include the following:

- Data held remotely can increase risk of loss of access to data due to network failure;
- There is a danger that access to agency data may be lost when contractual arrangements expire or cease between an agency and cloud service provider; and
- It can be difficult to access and audit the cloud computing provider to ensure that services provided meet requirements intended to prevent loss of access to data.

Cloud providers comprise an emergent sector. That means that some providers will undoubtedly fail or be required for financial reasons to alter their business model, perhaps reducing the functionality they offer in the process. This could result in the loss of access to vital business information.

Some cloud computing models have greater risks than others in relation to loss of access. The risk is less with IaaS especially as the agency will most likely have a copy of the data. With bankruptcy and receivership, the problem may be the amount of time to sort out and regain access to the data. Potential seizure of assets is an extension of this.

Mitigating risks related to loss of access to data include having plans in place to reduce the possibility of valuable business data being lost. Mitigation of risks may include the following:

- Determining what data the agency cannot afford to lose and ensuring that the data identified is not placed in a cloud environment;
- Requiring the service provider to notify the agency of any proposed change in ownership as part of the contractual obligations;
- Ensuring that data is always available by having several copies, including one held locally; and
- Ensuring that the risk of loss is low through having clear processes and regular auditing of cloud computing service and supply.

Plans may include performing due diligence when selecting a provider and ensuring that the agency's rights are clearly documented in contractual agreements and understood by both parties. Clauses in contracts may be used to ensure the agency's right to terminate the agreement, migrate to another service or fall back to a pre-cloud contract. A thorough selection process would look at the reputation and track record of the provider and their level of experience in implementing records management solutions in the cloud.

Clauses in contracts should specify that the cloud service provider:

- Creates and maintains proper back up systems;
- Demonstrates the effectiveness of their disaster recovery and business continuity plans to the agency on an agreed basis;
- Agrees to the agency's access requirements (such as ongoing business use or Freedom of Information requests);
- Agrees to notify the agency prior to any hardware or software upgrades. The notification period should take into account the time it would take for the agency to move to a new solution; and
- Implements disposal actions in line with agency specifications.

Continuity of service is likely to be disrupted at some point in time. Service level agreements should explicitly contain details about:

- Sufficient notification of and what constitutes scheduled downtime[18];
- Maintenance programmes, including definitions of complete and partial outages;
- Systems upgrades;
- Alternate arrangements for accessing data during prolonged outages; and
- Expected levels of uptime[19].

When identifying methods to prevent loss of access to data for cloud computing solutions, the following constraints must be met:

- Capture Principle 1: Full and accurate records of all agency activities and decisions are systematically created by authorised people or systems to meet business needs, accountability requirements and community expectations.
- Storage Principle 3: Public records must be stored away from known and unacceptable risk.
- Storage Principle 4: Public records must be stored in conditions that ensure their preservation for as long as the records are required, and the safety of the people handling the records.
- Strategic Management Principle 1: Responsibilities, authorities and accountabilities for records management must be clearly assigned, documented, communicated and assessed on an annual basis.
- Strategic Management Principle 4: Contracts, agreements or legislative instruments for outsourcing or privatisation must specify records management and monitoring practices that meet government and legislative records management requirements.
- Operations Management Principle 1: Recordkeeping procedures must cover all processes required to create and maintain full and accurate records consistently, adequately and appropriately.
- Operations Management Principle 2: All systems which contain public records must be effectively managed over their life, from acquisition to decommissioning, to ensure the system's integrity, reliability and performance quality.

[18] Downtime refers to periods of time when a system is unavailable.
[19] Uptime refers to periods of time when a system is available.

- Operations Management Principle 4: Recordkeeping frameworks, procedures and practices must be audited at least every two years to ensure the agency is operating in compliance with its' recordkeeping procedures.

The processes for the creation and maintenance of data stored and managed in a cloud computing environment are to be supported by documented procedures to meet the principles of *PROS 10/17 Operations Management Standard*. Procedures would include determining what data can be placed in the cloud, appropriate management of data in a cloud environment, and retrieval of data from a cloud.

Systems used to manage and store data in a cloud environment will need to be managed throughout their lifecycle to meet the principles of *PROS 10/17 Operations Management Standard*. This includes the decommissioning of systems and appropriate methods for the removal or migration of data.

Auditing cloud computing practice against the agency's recordkeeping requirements should be undertaken to meet the principles of *PROS 10/17 Operations Management Standard*. This includes audits of the service provider's recordkeeping practices undertaken on behalf of the agency as well as of agency practices.

Facilities and storage areas used to house Victorian government data must be authorised by the Keeper of Public Records to comply with *PROS 11/01 Storage Standard*. Where these facilities are commercially owned, the service provider must ensure that their facilities and storage areas are assessed under the Approved Public Record Office Storage Supplier (APROSS) Program. Cloud computing services run by a commercial third party are considered to be an APROSS and will need to be assessed and approved in accordance with this scheme. Regular inspection of APROSS facilities by a PROV representative is also required. The proposed APROSS facility must therefore be located within Victoria.

Where the cloud computing services are owned and operated by the agency (or Victorian Government), and therefore housed in an agency facility, the facility will need to be assessed by the agency representative for compliance with *PROS 11/01 S1 Agency Custody Storage Specification* as per Requirement 2 of that Specification.

There are a number of risks to data that are associated with cloud computing. The level of risk and possible consequences will need to be carefully assessed by the agency in order to determine whether the risks are unacceptable. Where there is an unacceptable level of risk, the agency must not use the cloud computing service. An alternative solution must be sought.

Systems used for cloud computing services must enable the data to be tracked, identified, and retrieved when required. Freedom of Information and other requests for data will need to be addressed efficiently and effectively, which can only occur in a cloud environment if the data is easily tracked, identified, and retrieved when required.

Agencies should ensure that the facilities used to store data in a cloud environment are regularly maintained. This includes support to maintain software applications, infrastructure, and hardware as well as early identification and mitigation of preservation risks for the data stored.

Disaster preparedness, management and recovery plans must cover data contained within a cloud environment. The longer that data stored in a cloud environment is unavailable the larger the impact on the agency's ability to conduct business, and the impact on individuals who need access to the data. The agency may be able to minimise the effect that a disaster will have by being aware of the anticipated level of impact, and the processes involved in managing a disaster before it occurs.

Any level of use of data stored by the agency in a cloud environment by the service provider will need to be determined to ensure that any conditions of use need to be conveyed.

Recommendations

Recommendation 9: PROV is proposing that agencies obtain evidence that the cloud service provider has had their internal controls and IT systems and processes independently audited to ensure a suitable standard of service delivery. This should be undertaken prior to the selection of the service provider, and at regular intervals throughout the provision of service. Audits should include the inspection and testing of services provided.

Auditing data management and systems is currently covered by the Operations Management Standard, and includes the following:

- New or upgraded systems have been acquired, developed or integrated to meet the agency's business needs and recordkeeping requirements (Operations Management Specification 1, Requirement 7).
- Processes and controls have been established to ensure the day-to-day reliability of systems for all users (Operations Management Specification 1, Requirement 8).
- Systems are monitored and maintained to ensure the integrity and performance quality of the system over their life (Operations Management Specification 1, Requirement 9).
- Recordkeeping procedures to be assessed by internal or external audits have been identified (Operations Management Specification 1, Requirement 16).
- A recordkeeping audit program has been developed and endorsed by the senior executive with recordkeeping responsibility (Operations Management Specification 1, Requirement 17).
- Recordkeeping audit procedures and criteria have been developed, and assessed following each audit (Operations Management Specification 1, Requirement 18).
- Results of recordkeeping audits and any audit recommendations have been documented, presented and reported to senior executives and relevant stakeholders (Operations Management Specification 1, Requirement 19).
- The progress of recordkeeping audit recommendations are monitored and reported to senior executives (Operations Management Specification 1, Requirement 20).

Implementing the above recommendation would be covered in a Guideline on how to implement the Standards in a cloud computing environment. The Guideline would fit under Storage. The *Operations Management Guideline 3: Recordkeeping and Systems Lifecycle Management* (currently under development) would be amended to refer to the cloud computing Guideline regarding managing systems within a cloud environment.

Questions

Q 4.2-1: Would there be any problem in implementing this recommendation in your agency?

Recommendations

Recommendation 10: PROV is proposing that agencies are able to demonstrate knowledge of what data is being stored in the cloud and the impact of it being unavailable for various periods of time.

Awareness of what data an agency manages is currently covered by the Capture and Storage Standards, and includes the following:

- An assessment has been undertaken to determine:
    - What types of records are to be created and captured by the agency; and

- The technology, systems, format and structure that business records are to be created and captured in (Capture Specification 3, Requirement 1).
- Processes have been developed and communicated to all staff (including volunteers and contractors) to ensure that records are complete, meaningful, consistent with legislative requirements and comprehensive, which cover:
  - What records are to be created and captured;
  - When records are to be created and captured;
  - What systems they are to be captured in;
  - Who are to create and capture them (this includes systems if records creation and capture is automated);
  - How records are to be created and captured; and
  - When a new version of a record is to be created, captured, and how it is to be identified (Capture Specification 3, Requirement 2).
- The minimum level of detail required to ensure that business records are complete, meaningful and comprehensive has been determined, built into processes and systems, and communicated to all staff (including volunteers and contractors) (Capture Specification 3, Requirement 3).
- Preservation risks have been identified, assessed and mitigated from the point of creation or capture as part of the agency's overall risk management framework (Capture Specification 3, Requirement 9).
- Systems for the intellectual control of public records within storage areas and facilities have been implemented to aid item level retrieval of records within storage containers (Storage Specification 1, Requirement 32).

The above recommendation would be covered in a Guideline on how to implement the Standards in a cloud computing environment. The Guideline would fit under Storage.

Questions

Q 4.2-2: Would there be any problem in implementing this recommendation in your agency?

Recommendations

Recommendation 11: PROV is proposing that agencies be required to keep a copy (such as a back up) of the data stored in a cloud in a separate location (that is, somewhere other than with the service provider).

Back up copies of agency data is currently covered by the Capture and Storage Standards, and includes the following:

- Preservation risks have been identified, assessed and mitigated from the point of creation or capture as part of the agency's overall risk management framework (Capture Specification 3, Requirement 9).
- The location of each storage area or facility has been subjected to a risk assessment to identify and mitigate possible risks to the preservation of and access to the public records stored there, and the results have demonstrated that the level of risk is low (Storage Specification 1, Requirement 10).

The above recommendation would be covered in a Guideline on how to implement the Standards in a cloud computing environment. The Guideline would fit under Storage.

Questions

Q 4.2-3: Would there be any problem in implementing this recommendation in your agency?

4.3 Inability to Ensure Data Integrity and Authenticity

The third recordkeeping issue with cloud computing is the means to ensure data integrity and authenticity. Such issues primarily occur in relation to SaaS. This is because the applications in PaaS and IaaS are the responsibility of the agency, which should ensure that requirements for data integrity are met. Lack of data integrity and authenticity could be by:

- Insufficient audit controls that make it difficult to accurately track what happened to the data when, or if the data has been altered and by who;
- Lack of appropriate metadata describing the contextual environment by which the data is managed; or
- No documented procedures or evidence that sequences of actions relating to data management are normal practice and in line with requirements.

Cloud applications may lack sufficient recordkeeping functionality, making it difficult or impossible for agencies to meet their records management obligations. This may include recordkeeping requirements contained in PROV's Standards and Specifications.

A change of ownership at a cloud provider could result in new owners not honouring previous contractual arrangements. Consequently, the agency may not know who has access to their information and the integrity of the data may be compromised.

It is important to ensure that data can be easily migrated to other providers (if the provider has gone out of business or because an agency wishes to change providers at the end of a contract). It should be established whether there are costs involved, what format the information will be exported in (such as an open format), and how long it will take before data can be accessed again.

Some cloud architectures do not have formal technical standards governing how data is stored and manipulated. This may lead to the inability for data to be successfully migrated to another system due to differences in the technical operating systems that manage and store the data.

The *PROS 11/07 Capture Standard* requires that authentic records be captured consistently by robust and compliant systems. Authenticity can be demonstrated by data resulting from comprehensive auditing processes and systems. Having these systems in place will enable agencies to know where their business data are and what actions are taking place.

To meet the principles in *PROS 11/07 Capture Standard* records must be created and kept of the actions and decisions related to storing and managing data in a cloud computing environment. This includes data created in a cloud computing environment. Procedures and systems automation are two methods that may be used.

Systems used to store and manage data in the cloud must be capable of consistently capturing records of agency activities and decisions. This includes activities such as who adjusted what data on what date and decisions such as why a particular data set was deleted or destroyed and who authorised its destruction.

Data created, stored and managed in a cloud computing environment must be able to link with their relevant context in order to ensure their reliability as evidence.

In order to ensure that data are preserved for the duration of their retention period, the formats and methods used to create and capture data in a cloud environment must be carefully assessed. If additional strategies are needed to ensure the preservation of the data,

the agency should ensure that the strategies have been identified and implemented. For example, the agency may need to state in the contract that the service provider keep and maintain agency data using an approved long-term preservation format.[20]

Data stored and managed in a cloud computing environment must be protected from unauthorised and undetected deletion.

Data migration is the transfer of data between storage types, formats or computer systems. It may be required when an agency moves to a new computer system or upgrades an existing system. In a cloud environment, a lack of portability standards may make it hard to remove business data to meet retention requirements at contract termination.

Metadata capture

Metadata is 'data describing context, content and structure of records and their management through time'.[21] Metadata helps ensure the authenticity and integrity of data by enabling them to be retrieved and interpreted more easily. It can support business processes and reflect the management of data over time.

Metadata issues associated with cloud computing includes the following:

- The functionality of the service provider's systems may not be sufficient to accommodate the required metadata fields or to enable future customisation; and
- Transactional metadata may not be automatically captured by the service provider's systems and associated with the relevant data.

Principal 2.1 of *PROS 11/09 Control Standard* states that metadata needed for the structure, context and management of business data is to be captured, maintained and connected with the data. It also states that 'the type and amount of metadata connected with a record will be limited by the boundaries of specific records, business and information systems'. Agencies would need to ensure that minimum metadata requirements are met and that it is possible to add customised metadata fields as required. Digital records can be connected with metadata in accordance with the Victorian Electronic Records Strategy (VERS).

Metadata is ideally assigned at point of creation, which may be prior to the data being stored with a service provider. Further transactional metadata will need to be captured at various additional points during the retention period and maintained for the duration of the records' lifecycle. This includes metadata elements regarding the business processes in which the data was used, the context of the management of the data and structural changes to the data (including its appearance).

The software, systems and infrastructure used for cloud computing must ensure the preservation of the data for the duration of the data's retention period. Preservation includes the ability for the data to be accessed and understood. Preservation must include the contextual metadata as well as the data concerned.

Under *PROS 10/10 S1 Strategic Management Specification* Requirement 22, contracted service providers must be required to comply with records management requirements determined by the agency. This should include any metadata, classification and tracking requirements needed for compliance with the *PROS 11/09 Control Standard*. Agencies will need to be able to locate and report on actions relating to data held in a cloud environment.

---

[20] Information about acceptable long-term preservation formats for electronic records is located in *PROS 99/007 Standard on the Management of Electronic Records*, which is available from PROV's website <http://prov.vic.gov.au/government/vers/standard-2/vers-specification-4>.
[21] AS ISO 15489:1, ss, 3, 12, p.3.

The minimum metadata set will need to be applied and the data will need to be classified in accordance with the agency's business classification schemes.

Agencies will need to specify to the cloud service provider's their responsibilities for creating and maintaining metadata. It should also be clear that the agency becomes the owner of all metadata at the end of the contract or if either party terminates the agreement. Cloud service agreements need to ensure that providers are aware of the importance of metadata to maintaining the integrity of the data and that metadata created as part of the operations of the cloud service provider remains the property of the agency.

Constraints regarding metadata and cloud computing includes the following:

- The requirements of Standards and Specifications associated with the Victorian Electronic Records Strategy (VERS).
- Operations Management Principle 1: Recordkeeping procedures must cover all processes required to create and maintain full and accurate records consistently, adequately and appropriately.
- Operations Management Principle 2: All systems which contain public records must be effectively managed over their life, from acquisition to decommissioning, to ensure the system's integrity, reliability and performance quality.
- Operations Management Principle 4: Recordkeeping frameworks, procedures and practices must be audited at least every two years to ensure the agency is operating in compliance with its' recordkeeping procedures.
- Capture Principle 1: Full and accurate records of all agency activities and decisions are systematically created by authorised people or systems to meet business needs, accountability requirements and community expectations.
- Capture Principle 2: Authentic records of all agency activities and decisions are consistently captured by robust and compliant systems.
- Capture Principle 3: Public records are correctly and clearly connected to the relevant times, people, systems, processes and events to ensure they are reliable evidence of what occurred.
- Capture Principle 5: Systems that capture public records maintain the integrity of the records as evidence, protecting them from undetected and unauthorised alteration.
- Control Principle1: Metadata elements needed for the structure, context and management of business records to be used and understood over time are captured, maintained and connected with the records.
- Control Principle 3: Business records are accurately tracked using systems that create, capture and maintain information about the movement of and actions on records.

Agencies should develop and implement procedures regarding creating and capturing records, recordkeeping controls, storing, accessing and disposing of records in the cloud.

Agencies should ensure that their cloud service provider has the ability to provide the required auditing and tracking services. Contract provisions regarding the lifecycle of the system, such as provisions for what happens when the system is decommissioned, may be used to manage the systems. The service provider may supply the agency with regular reports on the operations, design specifications and other documentation that demonstrates the reliability, integrity and performance quality of the systems used.

Agencies can mitigate risks by ensuring that contractual obligations regarding recordkeeping requirements are clearly specified and include migration of data. Contractual service provider agreements should clearly identify:

- The ownership of the data, including any intellectual property rights or copyright;

- Data migration requirements, including those to address the possible failure, expiration, or cessation of service agreements, or new ownership of the cloud. Does the data need to be migrated to a new provider or to the agency?
- The format that the data is to be migrated in.

Information gathered in auditing and tracking processes may include:

- Date and time of movement;
- Physical location of the data;
- Who has custody of the data;
- How and why the data was moved; and
- Actions taken place on the data.

4.4 Understanding the practical aspects of cloud services

Cloud computing is a relatively new term that is constantly being redefined as new technologies are created or augmented. There may be considerable differences in understanding what is meant by the term, which may have recordkeeping implications.

Software-as-a-service is usually defined as applications hosted in the cloud and accessed over the internet. A comprehensive understanding of what this means is needed to be able to assess the recordkeeping risks that may be involved. For example:

- Whose application is it? Is it the agency's application hosted in the cloud solely for their use? If so, would this constitute a private cloud scenario?
- Is it a shared application hosted 'in the cloud' where multiple clients share the same software code but each client's data is secure and not accessible by other clients? If so, does this constitute a public cloud scenario?
- In either of these scenarios, how would an agency go about confirming whether the system will adequately meet their recordkeeping requirements?

These questions have significant implications for recordkeeping issues as they directly impact the degree of control an agency will have over the applications and their data. The greater the level of control and input that an agency can have into the customisation and configuration of an application, the more likely they are to be able to meet their recordkeeping obligations.

When talking about customisation and configuration, what does this actually mean? What are the differences in difficulty between configuring an implementation on your own server compared with accessing an implementation configured on a cloud provider's server(s) through online access?

Agencies should conduct research to determine what they want from a cloud computing environment, and what a service provider can offer, to ensure that a shared, balanced and consistent understanding is reached by all parties.

Question

Q 4.4-1: Are the above issues problems for you?

Q 4.4-2: After reading this section, which of the above issues of cloud computing are most relevant to your agency?

Q 4.4-3: Are there other issues that PROV has not considered?

Q 4.4-4: What issues for your agency take precedent over the need to migrate to the cloud?

5. Summary

The transition to a cloud based service provider needs to be carefully considered as a risk based approach. Although PROV ideally would hope that agencies are able to maintain and service business records themselves, onsite and on premises or using Approved Public Record Office Storage Suppliers (APROSS) and Places Of Deposit (POD), PROV cannot ignore the ongoing cost associated with this initiative and the attractive alternative that cloud computing service providers may provide Victorian State and local government agencies. It is imperative that agencies ensure they are meeting their recordkeeping obligations under the Act and PROV's Standards and Specifications regardless of the environment. Agencies should anticipate the release of the *Recordkeeping Implications for Cloud Computing* policy.

Question

Q5-1: After reviewing this issues paper from PROV Is your agency still considering a move to the cloud environment?

Q5-2: Is your decision based on an assessment of the risks involved?

Q5-3: Will you be sourcing a provider from within Victoria or Australia?

Q5-4: If not what steps has your agency taken your to ensure the cloud service provider will comply with the requirements of PROV?

6. Definitions

The following terms are the major general recordkeeping terms of relevance for this paper. For terms specific to cloud computing, see Section 2. For a full list of records management and PROV terminology, see the *Master Glossary*.

Authenticity

'An authentic record is one that can be proven:

- To be what it purports to be;
- To have been created and sent by the person who purported to have created and sent it; and
- To have been created or sent at the time purported.'[22]

Disposal

A range of processes associated with implementing appraisal decisions which are documented in disposal authorities or other instruments. These include the retention, destruction or deletion or records in or from recordkeeping systems. They may also include the migration or transmission of records between recordkeeping systems, the transfer of ownership or the transfer of custody of records, e.g., to Public Record Office Victoria.

Due Diligence

a thorough investigation or audit of the cloud service provider, prior to signing the contract.

Government Agency

Any department, agency or office of the Government of Victoria.[23] It includes:

- Any department branch or office of the Government of Victoria;
- Any public statutory body corporate or unincorporated;
- A State-owned enterprise within the meaning of the State Owned Enterprises Act 1992;
- Any municipal council;
- Any other local governing body corporate or unincorporated; and
- Any Victorian court or person acting judiciously.

Integrity

'The integrity of a record refers to its being complete and unaltered.'[24]

Keeper of Public Records

The Keeper is the Director of Public Records Office Victoria. The Keeper of Public Records ('the Keeper') is responsible for the establishment of Standards for the efficient management of public records and for assisting agencies to apply those Standards to records under their control.[25]

Permanent Records

A public record which has been appraised by the Keeper of Public Records as required to be kept as part of Victoria's State Archives. Permanent records are specified in *Retention & Disposal Authorities* issued by the Keeper.

---

[22] Standards Australia, *AS ISO 15489 Australian standard on records management*, Standards Australia, Sydney, 2002, p. 7.
[23] *Public Records Act 1973*, s. 2
[24] *AS ISO 15489*, p. 7.
[25] *Public Records Act 1973*, ss. 6-7.

Personal Information	Information or an opinion that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can be reasonably ascertained, from the information or opinion.[26]
Public Record	(a) any record made or received by a public officer in the course of his duties; and (b) any record made or received by a court or person acting judicially in Victoria— but does not include— (c) a record which is beneficially owned by a person or body other than the Crown or a public office or a person or body referred to in s. 2B [of the Public Records Act 1973]; or (d) a prescribed record held for the purpose of preservation by a public office to which it was transferred before the commencement of the Arts Institutions (Amendment) Act 1994 by a person or body other than the Crown or a public office; or (e) a record, other than a prescribed record, held for the purpose of preservation by a public office to which it was transferred, whether before or after the commencement of the Arts Institutions (Amendment) Act 1994, by a person or body other than the Crown or a public office.[27]
Reliability	'A reliable record is one whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.'[28]
State Archives	Records identified as being of permanent significance to the government and people of Victoria and maintained and controlled by Public Records Office Victoria.
System	'Information system which captures, manages and provides access to records through time.'[29]
Transfer (Custody)	Change of custody, ownership and/or responsibility for records.[30]
Useability	'A useable record is one that can be located, retrieved, presented and interpreted.'[31]

[26] State Records Authority of New South Wales, *Guideline 12: Implementing a disposal authority*, State Government of NSW, Sydney, 2004.
[27] *Public Records Act 1973*, s. 2.
[28] *AS ISO 15489*, p. 7.
[29] *AS ISO 15489*, p. 3
[30] *AS ISO 15489:1*, s. 3.20.
[31] *AS ISO 15489*, p. 7.

7. Appendix Two: Federal Government Strategy

The Australian Federal Government has been circumspect in its approach of adopting cloud computing, due to their uncertainty over storing data in offshore data centres[32]. Given the decline in ICT budgets attributed to the economic crises, a number of Federal government agencies have adopted specific cloud computing services. The following agencies have undertaken work involving cloud computing:

- Australian Taxation Office (ATO) has moved eTax, Electronic Lodgement System (ELS) and Tax Agent Board administrative support systems into the cloud.
- Australian Bureau of Statistics has implemented a virtualization solution to enable transition to a private cloud environment.
- Treasury / ATO has migrated Standard Business Reporting (SBR) and Business Names projects into the Cloud.
- Department of Immigration and Citizenship (IMMI) initiated a proof of concept for the provisioning of an end-to-end online client lodgement process on a cloud platform.
- Australian Maritime Safety Authority has implemented a Public Cloud for SaaS and PaaS deployments from Salesforce.com.
- Department of Immigration and Citizenship (DIAC) has implemented a Hybrid Cloud for IaaS as a proof of concept.
- West Australian Health has opted for a private cloud for IaaS deployment. The data centres are expected to be completed mid 2011.

In terms of a more broad-based adoption, the Federal government has recently put together a framework to guide its cloud computing strategy. The Australian Federal Government has already adopted a Whole of Government approach toward data centres to consolidate all its data centres requirements for the next 10-15 years with an expected savings of $1 billion during that time period.

The Federal Government has adopted a three step process:

- Enabling (Early 2011 onwards). This consists of establishing a Cloud Information Community to facilitate knowledge sharing and monitor international adoption trends, and preparing the Whole of Government Cloud adoption framework.
- Public Cloud (Early 2011 onwards). This consists of increasing adoption of the Public Cloud owing to maturing of services (public facing websites, such as data.australia.gov.au, www.data.gov.au, are to be the first to be transitioned). Based on its performance, government will identify a panel of Cloud service providers.
- Private and Community Clouds (2012 onwards). This consists of integration of the Data Centre strategy with the Cloud Strategy, and establishing a Whole of Government Cloud storefront adoption of Private and Community Clouds based on costs and risks analysis.

[32] http://www.egov.vic.gov.au/trends-and-issues/information-and-communications-technology/cloud-computing.html

8. References

Australian Recordkeeping Initiative (ADRI) 2010, *Advice on managing the recordkeeping risks associated with cloud computing*, ADRI, Canberra, <http://www.adri.gov.au/products/Advice%20on%20managing%20the%20recordkeeping%20risks%20associated%20with%20cloud%20computing.pdf>.

Department of Business and Employment 2011, *Cloud computing and recordkeeping*, Department of Business and Employment, Darwin.

Department of Defence 2011, *Cloud Computing Security Considerations,* Australian Government, Canberra.

Hurwitz J, Bloor R, Kaufman M, Halper F 2010, *Cloud Computing for Dummies*, Wiley Publishing, Inc., New Jersey.

Lateral Economics 2011, *The potential for cloud computing services in Australia*, Lateral Economics, Melbourne.

National Archives of Australia 2011, *Outsourcing digital data storage*, NAA, Canberra, <http://www.naa.gov.au/records-management/agency/secure-and-store/naa-storage/outsourcing-digital-data-storage/index.aspx>.

National Archives of Australia 2011, *Records management and the cloud*, NAA, Canberra, <http://www.naa.gov.au/records-management/agency/secure-and-store/naa-storage/rm-cloud/index.aspx>.

National Archives of Australia 2011, *A Checklist for records management and the cloud*, NAA, Canberra, <http://www.naa.gov.au/Images/Cloud_checklist_with_logo_and_cc_licence_tcm16-44279.pdf>.

Queensland State Archives 2010, Managing the recordkeeping risk associated with cloud computing, Queensland State Archives, Brisbane, <http://www.archives.qld.gov.au/publications/publicrecordsbriefs/managing_recordkeeping_risks_cloud_computing.pdf >.

State Records NSW 2011, *Managing recordkeeping risk in the cloud*, State Records, State Records NSW, Sydney, <http://futureproof.records.nsw.gov.au/wp-content/uploads/2010/06/Managing-recordkeeping-risk-in-the-cloud.pdf>.

Williams, Dr Mark I, 2010, *A Quick Start Guide to Cloud Computing, Moving your Business into the Cloud,* Anthony Rowe Publishing, United Kingdom.

Legislation

Crimes Act 1958 (Victoria)

Evidence Act 1958 (Victoria)

Freedom of Information Act 1982 (Victoria)

Health Records Act 2001 (Victoria)

Information Privacy Act 2000 (Victoria)

Local Government Act 1989 (Victoria)

Occupational Health and Safety Act 2004 (Victoria)

Public Administration Act 2004 (Victoria)

Public Records Act 1973 (Victoria)

All current Victorian legislation is available at http://www.legislation.vic.gov.au

Standards

Public Record Office Victoria (PROV) 2010, *Recordkeeping Standard PROS 10/10 Strategic Management*, PROV Melbourne Victoria.

Public Record Office Victoria (PROV) 2010, *Recordkeeping Standard PROS 10/13 Disposal*, PROV Melbourne Victoria.

Public Record Office Victoria (PROV) 2010, *Recordkeeping Standard PROS 10/17 Operations Management*, PROV Melbourne Victoria.

Public Record Office Victoria (PROV) 2011, *Recordkeeping Standard PROS 11/01 Storage*, PROV Melbourne Victoria.

Public Record Office Victoria (PROV) 2011, *Recordkeeping Standard PROS 11/07 Capture*, PROV Melbourne Victoria.

Public Record Office Victoria (PROV) 2011, *Recordkeeping Standard PROS 11/09 Control*, PROV Melbourne Victoria.

Public Record Office Victoria (PROV) 2011, *Recordkeeping Standard PROS 11/10 Access*, PROV Melbourne Victoria.

Other Resources

For more information about recordkeeping, please contact:

Government Services
Public Record Office Victoria
Ph: (03) 9348 5600
Fax: (03) 9348 5656
Email: agency.queries@prov.vic.gov.au
Web: www.prov.vic.gov.au